IT SECURITY POLICY
EFFECTIVE MAY 1, 2017

ACACIA ENERGY GROUP
WWW.ACACIAENERGYGROUP.COM

2017

# IT SECURITY POLICY

ACACIA ENERGY GROUP

SWITZERLAND | MALTA | NETHERLANDS | USA | UK

Acacia

## Message from the Founder, President & CEO

Acacia Energy Group fully recognizes that information assets constitute important management resources, essential to conducting our business. We also acknowledge that it is absolutely imperative for our people and organization to be proactive in - and committed to - maintaining a high level of security so as to protect our information assets against any potential threat, by ensuring physical and technical security measures are firmly in place.

Today we face increasing threats from cyber attacks, loss of privacy and identity theft and fraud. We are dependent on secure, reliable and efficient information security systems. With that in mind, we established the Information Technology (IT) Security Policy that provides administrative rules and guidelines for the protection and proper utilization of our information technology assets.

Our IT Security Policy formalizes our information technology security program and creates a united effort across all Acacia office and production locations worldwide to protect the integrity of critical information. It is essential that we take a thorough and collaborative approach to managing our cyber and information technology security risks.

Please join the efforts to make our cyber security a reality. As this effort matures, you will see new Acacia's information technology security initiatives that will rely upon your involvement. Please be on the lookout for additional details.

All Acacia officers and employees shall have a good understanding of the Policy and perform their share of duties to maintain information technology security accordingly. It is my expectation that all of you will make time for this important part of our cyber security efforts.

Thank you for your ongoing and continuous efforts to maintain a safe and secure information technology environment.

**James W. Head**
Founder, President & CEO
Acacia Energy Group

# TABLE OF CONTENTS

# INTRODUCTION

This Information Technology (IT) Security Policy encompasses all aspects of security surrounding confidential company information and must be distributed to all company employees. All company employees must read this document in its entirety and sign the form confirming they have read and understand this policy fully. This document will be reviewed and updated by Acacia management on an annual basis or when relevant to include newly developed security standards into the Policy.

The use of computer systems and the exchange of information electronically have been increasing rapidly. Within the Acacia Energy Group there is a growing reliance on computer systems to run operations, expand communications, and improve our management and control. This growing dependence comes at a time when the number of threats and actual attacks on computer systems is constantly increasing. Information is one of our most important assets and each one of us has a responsibility to ensure the security of this information. Accurate, timely, relevant and adequately protected information is essential to the successful operations of the Acacia Energy Group.

The purpose of this IT Security Policy and its supporting policies, standards and guidelines is to define the security controls necessary to safeguard Acacia information systems and ensure the security, confidentiality, availability and integrity of the information held therein.

This Policy applies to all employees of Acacia Energy Group, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services. Compliance with policies in this document is mandatory for this constituency.

Exceptions to the policies defined in any part of this IT Security Policy may only be authorized by the Acacia’s Information Security Officer. In those cases, specific procedures may be put in place to handle requests and authorizations for exceptions. Every time a policy exception is invoked, an entry must be made into a security log specifying the date and time, description, reason for the exception and how the risk was managed.

# IT ASSETS

Acacia Energy Group handles sensitive information daily. Sensitive Information must have adequate safeguards in place to protect privacy and ensure compliance with various regulations.

Acacia is committed to respecting the privacy of all its customers and protecting any data about the customers from outside parties. The IT Security Policy defines the requirements for the proper and secure handling of all the IT assets in the Acacia Energy Group.

The IT Assets' policies apply to desktops, laptops, printers, smart phones, tablets, and other equipment, to applications and software, to anyone using those assets including internal users, temporary workers and visitors, and to any resource and capabilities involved in the provision of the IT services in general.

## IT Assets Policies

- All IT assets must only be used in connection with the assigned and/or authorized business activities.
- All IT assets must be classified into categories of the Acacia's business functions and security classification categories.
- Users are responsible for the protection and correct use of the IT assets that have been assigned to them.
- All IT assets must be in locations with security access restrictions, proper environmental conditions and workstations layout according to the security classification and technical specifications of the assets.
- Active desktops and laptops must be secured if left unattended.
- Access to the IT assets is forbidden for non-authorized personnel. Granting access to the IT assets involved in the provision of a service must be done through the approved Service Request and Access Management processes.
- All personnel interacting with the IT assets must have the proper training.
- Users shall maintain the IT assets assigned to them clean and free of accidents or improper use.
- Access to the IT assets must be restricted and properly authorized, including those employees accessing remotely. Company's laptops, PDAs and other equipment used at external locations must be periodically checked and maintained.

- The IT personal is solely responsible for maintaining and upgrading computer equipment configurations. The regular users are not authorized to change or upgrade configuration of the IT assets. That includes modifying hardware or installing software.
- Special care must be taken for protecting laptops, PDAs and other portable assets from being stolen. Users must be aware of extreme temperatures, magnetic fields and damages.
- When travelling by plane, portable equipment like laptops and PDAs must remain in possession of the user as handheld luggage.
- Whenever possible, encryption and erasing technologies should be implemented in portable assets in case they were stolen.
- Losses, theft, damages, tampering or other incidents related to the IT assets that compromise security must be reported as soon as possible to the Information Security Officer.
- Disposal of the IT assets must be done according to specific procedures for the protection of the information.
- IT assets storing confidential information must be physically destroyed in the presence of an Information Security Team member.
- IT assets storing sensitive information must be completely erased in the presence of an Information Security Team member before disposal.

## SENSITIVE DATA

Acacia’s sensitive information must be protected from an unauthorized access to safeguard the privacy and security of employees or the company. This policy applies to all Acacia’s users, including temporary users, visitors with temporary access, services providers and partners with limited or unlimited access time to services.

### Sensitive Data Policies

- Handle the Acacia information in a manner that corresponds with their sensitivity.
- Limit personal use of the Acacia information and telecommunication systems, and ensure it doesn’t interfere with employee’s job performance.
- Acacia reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose.
- Do not use email, Internet and other Acacia’s resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, indecent, obscene, harassing or illegal.

- Protect and do not disclose personnel information unless authorized.
- Keep passwords and accounts secure.
- Request approval from the management prior to installing any new software or hardware, third party connections, etc.
- Do not install unauthorized software or hardware, including modems and wireless access without specific management approval.
- Always leave workstations clear of sensitive data and lock computer screens when unattended.
- Information security incidents must be reported without delay.

## ACCEPTABLE USE

Acacia's sensitive information must be protected from an unauthorized access to safeguard the privacy and security of employees or the company. This policy applies to all Acacia's users, including temporary users, visitors with temporary access, services providers and partners with limited or unlimited access time to services.

### Acceptable Use Policies

- Acacia will maintain an approved list of technologies and devices, and personnel with the access to restricted devices.
- Employees are responsible for exercising good judgment regarding the personal use of company's devices.
- Employees must ensure that they have appropriate credentials and are authenticated for the use of Acacia's technologies and equipment.
- Employees should take all necessary steps to prevent unauthorized access to confidential data.
- Employees must ensure that technologies and equipment are used and set up in acceptable network locations.
- Employees must keep passwords secure and do not share their accounts.
- Authorized users are responsible for the security of their passwords and accounts.
- All PCs, laptops and workstations should be secured with the password-protected screensaver with the automatic sleep activation feature.
- All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered with or altered.
- Because information contained on portable computers is especially vulnerable, special care should be exercised.

- Postings by employees from a company's email address to social media and newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the company, unless posting is in the course of Acacia's business duties.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses and malicious code.

## NETWORK SECURITY

Acacia's network security policy consists of the practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of Acacia's computer network and network-accessible resources. This policy applies to all Acacia's users, including temporary users, visitors with temporary access, service providers and partners with limited or unlimited access time to services.

### Network Security Policies

- Firewalls must be implemented at each Internet connection and any internal company network.
- A network diagram detailing all inbound and outbound connections must be maintained and reviewed every 6 months.
- A firewall and router configuration document must be maintained which includes a documented list of services, protocols and ports including a business justification.
- Firewall and router configurations must restrict connections between untrusted networks.
- Firewall technology must be implemented where the Internet enters the company card network to mitigate known and on-going threats. Firewalls must also be implemented to protect local network segments and the IT resources that are connected to those segments such as the business and open networks.
- All inbound and outbound traffic must be restricted to what is required for the data environment.
- All inbound network traffic is blocked by default, unless explicitly allowed and the restrictions have to be documented.
- All outbound traffic has to be authorized by the office security management (i.e. whitelisted category of websites that can be visited by employees) and the restrictions have to be documented.
- Acacia's IT department will quarantine wireless users into a DMZ, where they will be authenticated and firewalled as if they were coming in from the Internet.
- Disclosure of private IP addresses to external entities must be authorized.

- A topology of the firewall environment has to be documented and has to be updated in accordance to the changes in the network.
- The firewall rules will be reviewed on a six months basis to ensure validity, and the firewall has to have a clean up rule at the bottom of the rule base.
- No direct connections from Internet to Acacia's data environment will be permitted. All traffic has to go through a firewall.

## ACCESS CONTROL

The Acacia's Access Control Policy defines the requirements for the proper and secure control of access to Acacia's IT services and infrastructure. This policy applies to all Acacia's users, including temporary users, visitors with temporary access, service providers and partners with limited or unlimited access time to services.

### Access Control Policies

- Any system that handles valuable information must be protected with a password-based access control system.
- Any system that handles confidential information must be protected by a two-factor authentication access control system.
- Discretionary access control list must be in place to control the access to resources for different groups of users.
- Mandatory access controls should be in place to regulate access by process operating on behalf of users.
- Access to resources should be granted on a per-group basis rather than on a per-user basis.
- Access shall be granted under the principle of "less privilege", i.e., each identity should receive the minimum rights and access to resources needed for them to be able to perform successfully their business functions.
- Whenever possible, access should be granted to centrally defined and centrally managed identities.
- Users should refrain from trying to tamper or evade the access control in order to gain greater access than they are assigned.
- Automatic control scan technologies and periodic revision procedures must be in place to detect any attempt made to circumvent controls.

# PHYSICAL SECURITY

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorized individuals from obtaining sensitive data. This policy applies to all Acacia's users, including temporary users, visitors with temporary access, service providers and partners with limited or unlimited access time to services.

## Physical Security Policies

- Employees are responsible for exercising good judgment regarding the personal use of Acacia's IT equipment.
- Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies.
- Employees should take all necessary steps to prevent unauthorized access to confidential data.
- Employees should ensure that technologies are used and setup in acceptable network locations.
- A list of devices that accept payment card data should be maintained.
- A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the Acacia's premises for a short duration, usually for no more than one day.
- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
- Media is defined as any printed or handwritten paper, received faxes, flash drives, back-up drives, computer hard drives, etc.
- Media containing sensitive information must be handled and distributed in a secure manner by trusted individuals.
- Visitors must always be escorted by a trusted employee when in the areas that hold sensitive information.
- Procedures must be in place to help all personnel to easily distinguish between employees and visitors, especially in the areas where sensitive data is accessible. "Employee" refers to full-time and part-time employees, temporary employees and personnel, and consultants who are "resident" on the Acacia's sites. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually for no more than one day.
- Network jacks located in public areas and accessible to visitors must be disabled and enabled when network access is explicitly authorized.

- All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
- Strict control is maintained over the external or internal distribution of any media containing sensitive data and has to be approved by the security office management.

## PASSWORD CONTROL

Acacia's Password Control Policy defines the requirements for the proper and secure handling of passwords in the company. This policy applies to all Acacia's users, including temporary users, visitors with temporary access, services providers and partners with limited or unlimited access time to services.

### Password Control Policies

- Any system that handles valuable information must be protected with a password-based access control system.
- Every user must have a separate, private identity for accessing Acacia IT network services.
- Identities should be centrally created and managed. Single sign-on for accessing multiple services is encouraged.
- Each identity must have a strong, private, alphanumeric password to be able to access any service. They should be as least 8 characters long.
- Each regular user may use the same password for no more than 90 days and no less than 3 days. The same password may not be used again for at least one year.
- Password for some special identities will not expire. In those cases, password must be at least 15 characters long.
- Use of administrative credentials for non-administrative work is discouraged. Acacia's IT administrators must have two sets of credentials: one for administrative work and the other for common work.
- Sharing of passwords is forbidden. They should not be revealed or exposed to public.
- Whenever a password is deemed compromised, it must be changed immediately.
- For critical applications, digital certificates and multiple factor authentication, smart cards should be used whenever possible.
- Identities must be locked if password guessing is suspected on the account.

# EMAIL USE

Acacia’s Email Policy defines the requirements for the proper and secure use of electronic mail in the company. This policy applies to all Acacia’s users, including temporary users, visitors with temporary access, service providers and partners with limited or unlimited access time to services.

## Email Use Policies

- All assigned email addresses, mailbox storage and transfer links must be used only for business purposes. Occasional use of personal email address using Acacia’s Internet access may be permitted if there is no significant consumption of Acacia’s system resources and employee’s work duties are not affected.
- Use of Acacia’s resources for non-authorized advertising, external business, spam, political campaigns, and other non-business related uses are strictly prohibited.
- Use of Acacia’s email resources for disseminating messages regarded as offensive, racist, obscene or in any way contrary to the law and ethics is absolutely discouraged.
- Use of Acacia’s email resources is allowed only to the extent and for the time is needed for performing the duties. When a user ceases his/her relationship with the company, the associated account must be deactivated according to established procedures for the lifecycle of the accounts.
- Users must have private identities to access their emails and individual storage resources, except specific cases where common usage may be deemed appropriate.
- Privacy is not guaranteed. When strongest levels of confidentiality, authenticity and integrity are required, use of electronically signed messages is encouraged. However, only the Information Security Officer may approve the interception and disclosure of messages.
- Identities for accessing corporate email must be protected by strong passwords. The complexity and lifecycle of passwords are managed by Acacia’s procedures for managing identities. Sharing of passwords is discouraged. Users should not impersonate another users.
- Outbound email messages from corporate users should have approved signatures at the bottom of the email message.
- Attachments must be limited in size according to specific instructions of Acacia’s IT department. Whenever possible, restrictions should be automatically enforced.
- Scanning technologies for viruses and malware must be on users’ PCs and servers to ensure the maximum protection of the incoming and outgoing email.

- Security incidents must be reported and handled as soon as possible. Users should not try to respond by themselves to security attacks.
- Corporate mailboxes content should be centrally stored in locations where the information can be backed up and managed according to company procedures.
- Purge, backup and restore functions must be managed according to specific instructions of Acacia's IT department.

## INTERNET USE

Acacia's Internet Usage Policy applies to all employees who have access to computers and the Internet to be used in the performance of their work. Use of the Internet by employees is permitted and encouraged where such use supports the goals and objectives of the business.

However, access to the Internet through Acacia's network is a privilege and all employees must adhere to the policies concerning Internet usage. Violation of these policies could result in disciplinary and/or legal action leading up to and including termination of employment.

Employees may also be held personally liable for damages caused by any violations of this policy. All employees are required to acknowledge receipt and confirm that they have understood and agree to abide by the Internet use rules rules hereunder.

### Internet Use Policies

- Acacia employees are expected to use the Internet responsibly and productively. Internet access is limited to job-related activities only and personal use is not permitted.
- All Internet data that is composed, transmitted and/or received by Acacia's computer systems is considered to belong to Acacia and is recognized as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties.
- The equipment, services and technology used to access the Internet are the property of Acacia and the company reserves the right to monitor Internet traffic and monitor and access data that is composed, sent or received through its online connections.
- All sites and downloads may be monitored and/or blocked by Acacia if they are deemed to be harmful and/or not productive to business.
- The installation of software such as instant messaging technology is strictly prohibited.

### Unacceptable use of the Internet by employees includes, but is not limited to:

- Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via Acacia’s email service.
- Using computers to perpetrate any form of fraud, and/or software, film or music piracy.
- Stealing, using, or disclosing someone else's password without authorization.
- Downloading, copying or pirating software and electronic files that are copyrighted or without authorization.
- Sharing confidential material, trade secrets, or proprietary information outside of the organization.
- Hacking into unauthorized websites.
- Sending or posting information that is defamatory to the company, its products and services, colleagues and/or customers.
- Introducing malicious software onto the company network and/or jeopardizing the security of the organization's electronic communications systems.
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities.
- Passing off personal views as representing those of the organization.

## ANTIVIRUS SOFTWARE

Acacia’s Antivirus Policy defines the requirements for the proper implementation of antivirus software and other forms of protection in the organization. This policy applies to servers, workstations and equipment in the organization, including portable devices like laptops and PDAs that may travel outside of the organization facilities. Some policies apply to external computers and devices accessing the resources of the organization.

### Antivirus Software Policies

- All computers and devices with access to the Acacia’s network must have an antivirus client installed, with real-time protection.
- All servers and workstations owned by Acacia or permanently in use in the Acacia’s facilities must have approved and centrally managed antivirus software. That also includes travelling devices that regularly connects to the Acacia’s network or that can be managed via secure channels through Internet.

- Acacia’s computers permanently working in other organization’s network may be exempted from the previous rule if required by the security policies of other organization, provided those computers will be protected as well.
- Traveling Acacia’s computers that seldom connect to the Acacia’s network should have installed approved and independently managed antivirus software.
- All installed antivirus software must automatically update virus definitions. They must be monitored to ensure successful updating is taken place.
- Visitors’ computers and all computers that connect to the Acacia’s network are required to stay “healthy”, i.e. with valid, updated antivirus software installed.

## INFORMATION CLASSIFICATION

The Acacia’s Information Classification Policy defines a framework for the classification of the information according to its importance and risks involved. It is aimed at ensuring the appropriate integrity, confidentiality and availability of the Acacia’s information. This policy applies to all the information created, owned or managed by Acacia, including information stored in electronic or magnetic forms and printed on paper.

### Information Classification Policies

- Information owners must ensure security of their information and systems that support it.
- Acacia’s Information Security management is responsible for ensuring confidentiality, integrity and availability of the Acacia’s assets, information, data and IT services.
- Any breach must be reported immediately to the Information Security Officer. If needed, the appropriate countermeasures must be activated to assess and control damages.
- Acacia’s information is classified according to its security impact. The current categories are: confidential, sensitive, shareable, public and private.
- Information defined as confidential has the highest level of security. Only a limited number of people have access to it. Management, access and responsibilities for confidential information must be handled with special procedures defined by Information Security management.
- Information defined as sensitive may be handled by a greater number of persons. It is needed for daily performance of jobs duties, but should not be shared outside of the scope needed for the performance of the related work functions.

- Information defined as shareable can be shared outside of Acacia, for those clients, organizations, regulators, etc. who acquire or should get access to it.
- Information defined as public can be shared in public domain, e.g. content published on the company's website.
- Information deemed as private belongs to individuals who are responsible for the maintenance and backup.
- The Information Security Officer and the information owner classify information jointly.

## REMOTE ACCESS

Acacia's Remote Access Policy defines the requirements for the secure remote access to the Acacia's internal resources. This policy applies to the users and devices that need access to the Acacia's internal resources from remote locations.

### Remote Access Policies

- To gain access to the Acacia's internal resources from remote locations, users must have the required authorization. Remote access for the employee, external user or partner can be requested only by the Manager responsible for the information and granted by the Access Management.
- Only secure channels with mutual authentication between server and clients must be available for remote access. Both server and clients must receive mutually trusted certificates.
- Remote access to confidential information should not be allowed. Exceptions are authorized only on the case-by-case basis.
- Users must not connect from public computers unless the access is for viewing public content.

## OUTSOURCING

Acacia's Outsourcing Policy defines the requirements needed to minimize risks associated with the outsourcing of IT services, functions and processes. This policy applies to the organization, services providers, IT services, functions or processes that have been outsourced, and outsourcing process itself.

### Outsourcing Policies

- Before outsourcing any service, function or process, a careful strategy must be followed to evaluate the risk and financial implications.
- Whenever possible, a bidding process should be used to select between several service providers.

- In any case, the service provider should be selected after careful evaluation of their reputation, experience in service to be provided, offers and warranties.
- Audits should be planned in advance to evaluate performance of the service provider before and during the provision of the outsourced service, function or process.
- If the organization doesn't have enough knowledge and resources, a specialized company should be hired to do the auditing.
- A service contract and defined service levels must be agreed between the Acacia and the service provider.
- The service provider must obtain an authorization from Acacia if it intends to hire a third party to support the outsourced service, function or process.

## IT ROLES AND RESPONSIBILITIES

Roles and responsibilities of Acacia's IT department are listed below.

### Chief Information Officer

- Accountable for all aspects of the Acacia's information security

### Information Security Officer

- Responsible for the security of the IT infrastructure
- Planning against security threats, vulnerabilities, and risks
- Implementation and maintenance of Security Policy documents
- Supervision of security training programs
- Accountable for IT infrastructure supporting Security Policies
- Response to information security incidents and threats
- Help in disaster recovery plans

### Information Owners

- Help with the security requirements for their specific area
- Determine privileges and access rights to the resources within their areas

### IT Security Team

- Implements and operates IT security
- Implements the privileges and access rights to the resources
- Supports Security Policies

### Users

- Meet Security Policies
- Report any attempted security breaches

## DISCIPLINARY ACTIONS

Violation of the policies and procedures of this IT Security Policy will result in disciplinary actions, from warnings up to termination of employment. Claims of ignorance, good intentions or poor judgment will not be accepted as the excuses for non-compliance.

## NOTES

______________________________________________________________________

______________________________________________________________________

______________________________________________________________________

______________________________________________________________________

______________________________________________________________________

______________________________________________________________________

______________________________________________________________________

______________________________________________________________________

______________________________________________________________________

______________________________________________________________________

EMPLOYEE NAME: EMPLOYEE SIGNATURE: DATE:

WWW.ACACIAENERGYGROUP.COM

Acacia Energy Group

2017

# IT SECURITY POLICY

EFFECTIVE MAY 1, 2017

ACACIA ENERGY GROUP
SWITZERLAND | MALTA | NETHERLANDS | USA | UK